



## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets <sup>6</sup> : <b>G06F 1/00</b>	<b>A2</b>	(11) Numéro de publication internationale: <b>WO 97/07448</b> (43) Date de publication internationale: 27 février 1997 (27.02.97)
(21) Numéro de la demande internationale: PCT/FR96/01269 (22) Date de dépôt international: 8 août 1996 (08.08.96) (30) Données relatives à la priorité: 95/09952      21 août 1995 (21.08.95)      FR 95/13038      3 novembre 1995 (03.11.95)      FR (71)(72) Déposant et inventeur: SIRBU, Cornel [RO/FR]; 30, rue de l'Ecosse, F-78280 Guyancourt (FR). (74) Mandataire: BREESE MAJEROWICZ; 3, avenue de l'Opéra, F-75001 Paris (FR).	(81) Etats désignés: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, brevet ARIPO (KE, LS, MW, SD, SZ, UG), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).  Publiée <i>Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.</i>	

(54) Title: CONDITIONAL ACCESS METHOD AND DEVICE

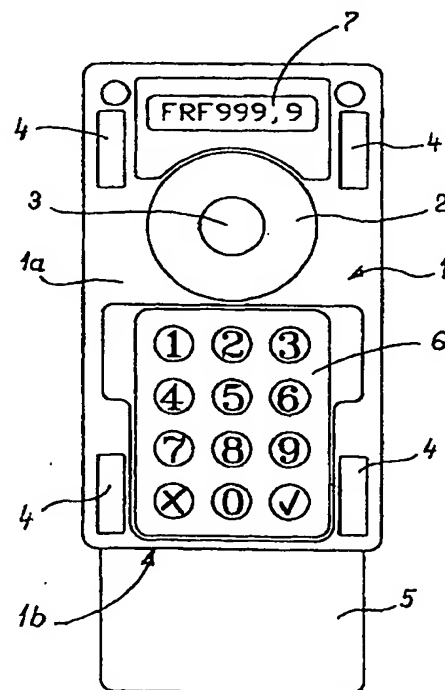
(54) Titre: DISPOSITIF ET PROCÉDE D'ACCES CONDITIONNEL

## (57) Abstract

The invention concerns a conditional access method and device for use in connection with a host electronic equipment, including a pointer peripheral containing one or more integrated circuit card coupler units, characterised in that said device also includes means for acquiring personal information concerning a user, and in that said personal information is locally compared with information stored in the integrated circuit card (5) without passing through the host equipment.

## (57) Abrégé

La présente invention concerne un dispositif et un procédé d'accès conditionnel destiné à être utilisé en liaison avec un équipement électronique hôte, constitué par un périphérique de pointage incorporant au moins un coupleur de carte à microcircuit, caractérisé en ce qu'il incorpore en outre des moyens d'acquisition d'informations personnelles propres à un utilisateur et en ce que lesdites informations personnelles sont comparées localement avec les informations mémorisées dans la carte à microcircuit (5) sans que lesdites informations personnelles ne transitent par l'équipement hôte.



# **UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Arménie	GB	Royaume-Uni	MW	Malawi
AT	Autriche	GE	Géorgie	MX	Mexique
AU	Australie	GN	Guinée	NE	Niger
BB	Barbade	GR	Grèce	NL	Pays-Bas
BE	Belgique	HU	Hongrie	NO	Norvège
BF	Burkina Faso	IE	Irlande	NZ	Nouvelle-Zélande
BG	Bulgarie	IT	Italie	PL	Pologne
BJ	Bénin	JP	Japon	PT	Portugal
BR	Brsil	KE	Kenya	RO	Roumanie
BY	Bélarus	KG	Kirghizistan	RU	Fédération de Russie
CA	Canada	KP	République populaire démocratique de Corée	SD	Soudan
CF	République centrafricaine	KR	République de Corée	SE	Suède
CG	Congo	KZ	Kazakhstan	SG	Singapour
CH	Suisse	LI	Liechtenstein	SI	Slovénie
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovaquie
CM	Cameroun	LR	Libéria	SN	Sénégal
CN	Chine	LT	Lituanie	SZ	Swaziland
CS	Tchécoslovaquie	LU	Luxembourg	TD	Tchad
CZ	République tchèque	LV	Lettonie	TG	Togo
DE	Allemagne	MC	Monaco	TJ	Tadjikistan
DK	Danemark	MD	République de Moldova	TT	Trinité-et-Tobago
EE	Estonie	MG	Madagascar	UA	Ukraine
ES	Espagne	ML	Mali	UG	Ouganda
FI	Finlande	MN	Mongolie	US	Etats-Unis d'Amérique
FR	France	MR	Mauritanie	UZ	Ouzbékistan
GA	Gabon			VN	Viet Nam

**Dispositif et procédé d'accès conditionnel.***Domaine de l'invention*

5           La présente invention concerne un dispositif d'accès conditionnel formé par un périphérique de pointage intégrant un ou plusieurs coupleurs pour les cartes à microcircuit.

10           Le dispositif est destiné à la mise en oeuvre de transactions sécurisées par cartes à microcircuit, à l'identification du porteur de carte, et/ou au contrôle des étapes des transactions.

15           Les applications concernent notamment l'accès conditionnel aux ressources de l'équipement hôte, à l'accès conditionnel de ressources disponibles sur un équipement extérieur auquel l'équipement hôte est relié ou connecté, la gestion de licences d'exploitation de logiciels mémorisés sur l'équipement hôte ou sur des équipements extérieurs auxquels l'équipement hôte est relié ou connecté, le paiement  
20   électronique, etc.

*Définitions*

25           Par "carte à microcircuit" on entendra un support, généralement une carte, comportant un ou plusieurs circuits intégrés exécutant des fonctions de traitement et/ou de mémorisation, par exemple une carte à mémoire ou carte à microprocesseur communément appelée "cartes à puce", une carte sans contact ou une carte PCMCIA.

30           Par "coupleur de carte à microcircuit", on entendra tout moyen mettant en oeuvre une interface pour l'échange de signaux entre un matériel et la carte à microcircuit, selon des protocoles de communications standardisés ou spécifiques. L'échange de signaux peut être réalisé par une connexion  
35   électrique ou une liaison sans fil, par exemple électromagnétique, ou lumineuse.

## 2

Par "équipement hôte", on entend un terminal d'ordinateur, une station de travail, un ordinateur personnel, un terminal multimédia, etc. et particulièrement, mais non exclusivement, tout équipement susvisé comportant  
5 des moyens de connexion bidirectionnelle temporaire ou permanente à un réseau de communication local ou publique.

Par "périphérique de pointage", on entendra un dispositif actionné manuellement par son utilisateur pour agir sur des objets visuels, destiné à être utilisé avec un  
10 équipement hôte interactif comportant un écran et une interface utilisateur graphique comprenant les objets visuels, tels qu'une souris opto-mécanique à bille, une souris optique nécessitant un tapis spécial, une boule ou track-ball, un numériseur à stylet ou à curseur, un pointeur  
15 tactile, un manche ou joystick, une télécommande à levier pour CD-I.

*Etat de la technique*

20 Ces périphériques fonctionnent conjointement avec l'équipement qu'ils contrôlent et auquel ils sont connectés par l'intermédiaire d'un port de communication, par exemple un port RS232, USB ou équivalent, ou encore reliés par un moyen de transmission sans fil, par exemple par liaison  
25 infrarouge ou hertzienne. Dans certains cas, notamment lorsque l'équipement hôte est un ordinateur portable, ces périphériques sont intégrés dans ce dernier, bien qu'ils forment un équipement autonome.

Il s'agit généralement de dispositifs facilement  
30 interchangeables en raison de l'adoption par la plupart des constructeurs d'équipements hôtes de standards communs. Ces périphériques sont également des dispositifs d'un prix relativement faible par rapport au prix de l'équipement hôte. Ils peuvent donc être remplacés de façon indépendante de  
35 l'équipement hôte par un dispositif similaire sans inconvénient.

On a proposé dans l'état de la technique d'intégrer dans certains périphériques de pointage un connecteur de carte à microcircuit, par exemple dans les brevets européen EP485275 ou allemand DE4326735. Le périphérique décrit dans la demande de brevet européen EP485275 formant l'état de la technique le plus proche comporte un connecteur de carte à microcircuit directement relié aux conducteurs communs entre l'ordinateur et le périphérique, afin de permettre à la fois l'échange de signaux relatifs aux fonctions de pointage, et l'échange de signaux pour l'exploitation des fonctions de sécurité associées à la carte à microcircuit. Le périphérique se comporte de manière transparente entre la carte à microcircuit et l'ordinateur auquel il est connecté. Aucun traitement ne se fait au sein du périphérique, qui se contente d'assurer la liaison électrique entre la carte à microcircuit et l'ordinateur. L'ensemble du processus de saisie du code d'identification personnel se fait donc dans l'équipement hôte, ce qui n'est pas satisfaisant et constitue un inconvénient majeur pour le développement commercial des réseaux publics tels qu'INTERNET.

*Problème objectif de l'état de la technique*

En effet, les équipements hôtes sont aujourd'hui presque toujours reliés à au moins un réseau, soit interne à une organisation, soit publique, par exemple par INTERNET. Il est donc possible, voire facile, pour un tiers, de se connecter à l'équipement hôte et de prendre connaissance des informations traitées par ce dernier. Il existe bien des solutions techniques pour filtrer les informations accessibles par des tiers extérieurs, mais ces solutions sont en contradictions avec la volonté d'ouverture et d'augmentation du niveau de communication de la plupart des utilisateurs, et impose, pour un fonctionnement optimal, des arbitrages complexes et généralement hors de portée de l'utilisateur moyen.

*Exposé de l'invention*

L'objet de l'invention est de remédier à ces  
5 inconconvénients en proposant un dispositif d'accès conditionnel  
augmentant sensiblement le niveau de sécurité contre des  
intrusions abusives par des tiers tentant de se procurer le  
code ou la clé d'accès associées à la carte à microcircuit en  
se connectant à l'équipement hôte par un réseau publique ou  
10 interne. A aucun moment, une intrusion dans les mémoires de  
l'ordinateur ne permettra d'accéder aux données relatives à  
la certification de l'utilisateur.

A cet effet, l'invention réside dans le fait que  
l'exploitation de la carte à microcircuit se fait localement,  
15 c'est-à-dire dans le périphérique de pointage et non pas dans  
l'équipement hôte. Cette caractéristique est essentielle.  
Elle assure un cloisonnement entre les moyens  
d'identification de l'utilisateur d'une part, et l'ordinateur  
et le réseau de communication auquel il est ou peut être  
20 raccordé d'autre part.

Les moyens d'identification de l'utilisateur sont  
réunis dans le périphérique de pointage auquel seul  
l'utilisateur a accès. Il saisit les données personnelles en  
principe secrètes, par exemple son code confidentiel. Ces  
25 données sont vérifiées par un microcalculateur local avec les  
informations enregistrées par la carte. Ce microcalculateur  
est généralement intégré dans la carte à microcircuit, mais  
peut également être intégré dans le périphérique. Cette  
vérification n'entraîne dans les dispositifs et procédés  
30 selon l'invention aucune transmission de données secrètes  
vers l'ordinateur. La comparaison se traduit par une  
information d'agrément ou non de l'utilisateur, qui constitue  
la seule information transmise à l'ordinateur. Ceci est  
essentiel pour éviter l'accessibilité d'informations  
35 confidentielles telles que le code à un tiers relié à

l'ordinateur par l'intermédiaire d'un réseau local ou un réseau téléphonique.

*Caractéristiques additionnelles de l'invention*

5

L'invention est avantageusement complétée par les différentes caractéristiques suivantes :

- il comporte un capteur pour la saisie d'un signal d'identification biométrique, tel qu'un capteur d'images d'empreintes digitales et/ou un capteur d'images de fond de l'oeil et/ou un capteur de reconnaissance vocale ;
- il comporte des moyens de contrôle vocal d'une transaction ;
- le clavier et/ou l'écran est (sont) disposé(s) sur la face supérieure de la souris et en ce qu'un couvercle est articulé sur le boîtier de la souris pour, en position fermée, protéger ledit clavier et/ou ledit écran lorsque le coupleur de carte à puce n'est pas utilisé ;
- une fente d'introduction d'une carte à puce est prévue au niveau d'une rainure que présente la souris sur son pourtour dans le prolongement de l'espace entre des touches d'actionnement et un corps du boîtier de ladite souris sur lequel lesdites touches sont montées ;
- dans le cas où le périphérique comporte un capteur d'images d'empreintes digitales, son boîtier présente un guide destiné à recevoir un doigt de l'opérateur, par exemple son pouce ;
- le dispositif comporte une horloge à alimentation permanente permettant de dater les opérations, notamment les opérations financières ;
- il comporte au moins deux entrées de cartes à puce ;
- il comporte des moyens pour la gestion et l'exécution d'au moins une application de sécurité associée à un logiciel applicatif de l'équipement hôte ;
- il comporte des moyens permettant le transfert d'une application de sécurité entre des moyens de stockage,

gestion et exécution d'une application de sécurité et une carte à microcircuit comportant une application de distribution de ces applications de sécurité ;

- 5       • il constitue un presse-papiers à stylet et à double coupleur de carte à puce et comporte des moyens pour saisir, compresser et enregistrer des informations manuscrites et les décharger ultérieurement dans l'équipement hôte ;
- 10       • il constitue un assistant personnel multimédia et/ou incorpore des moyens mettant en oeuvre d'une ou plusieurs applications bureautiques telles qu'une calculatrice, un agenda, une horloge, etc. ;
- 15       • il comporte une horloge à fonctionnement permanent et des moyens pour transmettre à l'équipement périphérique des données numériques datées comportant une séquence de données relative à l'autorisation calculée à partir des données mémorisées dans la carte à microcircuit et des données saisies par l'utilisateur et une séquence de données délivrée par l'horloge.

20       L'invention concerne également un procédé pour la gestion et l'exécution d'application de sécurité dans l'équipement hôte consistant à procéder à la comparaison dans un périphérique relié à un équipement hôte de données personnelles et de données enregistrées dans une carte à  
25       microcircuit sans que les données personnelles ne soient transmises à l'équipement hôte, le périphérique intégrant des moyens d'acquisition des données personnelles et au moins un connecteur de carte à microcircuit.

30       Suivant un mode de mise en oeuvre avantageux, le procédé comprend un protocole de communication étendu du protocole de communication spécifique aux moyens de pointage du dispositif périphérique. Ce protocole permet l'utilisation d'un seul port série pour la communication entre des logiciels applicatifs et les moyens de pointage et les moyens  
35       sécurisés réunis dans le dispositif selon l'invention.

Ainsi, selon une forme avantageuse de ce protocole, les données et les commandes sont transmises sous la forme de trames comprenant un ensemble de champs constitué chacun d'une séquence codée comportant un nombre prédéterminé de bits, chaque trame comprenant un champ d'identification et au moins un des champs suivants :

- champ de l'information de pointage,
- champ de l'information relative aux moyens sécurisés.

Le champ l'information relative aux moyens sécurisés comporte obligatoirement un champ de contrôle qui précise le type d'information suivi des champs optionnels donnant la longueur du message d'application de sécurité, et un champ de contrôle d'intégrité dudit message.

Avantageusement, le procédé fournit l'information de pointage à un logiciel applicatif et en même temps assure la transmission des messages vers le même ou un autre logiciel applicatif simultanément actif et son application de sécurité.

De préférence, l'appareil transmet les messages émis par les moyens sécurisés sous la forme de trames dont le premier champ est la trame spécifique de pointage modifiée suivie dudit message complet ou répartit sur plusieurs trames du même type. Aussi, les trames de pointage et les trames étendues peuvent être alternées.

Selon une variante, les moyens sécurisés de stockage et d'exécution desdites applications de sécurité sont regroupés dans une carte à microcircuit miniature amovible. Ainsi, la gestion et la disponibilité desdits moyens de stockage et exécution des applications de sécurité sont rendues indépendantes de la maintenance du dispositif.

*Présentation des dessins annexés*

L'invention sera mieux comprise à la lecture de l'exposé détaillé suivant, donné à titre d'exemple non limitatif et illustré par les figures annexées :

- 5       - la figure 1 est une représentation en vue de dessous (côté bille) d'un dispositif d'accès conditionnel conforme à une réalisation possible de l'invention dans sa version "souris" ;
- 10       - les figures 2a et 2b sont des représentations en vue en perspective de deux variantes de réalisation possibles pour la souris de la figure 1 ;
- 15       - la figure 2c représente une vue d'un écran pour la mise en oeuvre d'une variante de réalisation ;
- la figure 3 est une représentation schématique illustrant une configuration avantageuse possible à l'intérieur du boîtier de la souris de la figure 1 ;
- 20       - la figure 4 est une vue de dessus d'un dispositif d'accès conditionnel de type souris à bille conforme à une autre variante de réalisation possible pour l'invention ;
- la figure 5 est une vue en perspective illustrant un mode de réalisation possible pour la variante de la figure 4 ;
- 25       - la figure 6 est une représentation schématique en vue de côté illustrant un mode de réalisation possible pour la variante de la figure 4 ;
- la figure 7 est un synoptique illustrant un dispositif d'accès conditionnel avec contrôle biométrique ;
- la figure 8 est une vue de dessus d'un dispositif d'accès conditionnel avec contrôle biométrique ;
- 30       - la figure 9 est une représentation schématique en perspective avec arraché d'un clavier de micro-ordinateur avec un dispositif tactile de pointage selon l'invention ;
- 35       - la figure 10 est un organigramme illustrant une séquence d'interrogation possible par un logiciel applicatif, d'une application de sécurité portée par une carte collectrice insérée dans un dispositif d'accès conditionnel conforme à un mode de réalisation possible pour l'invention ;

- les figures 11 et 12 sont des organigrammes illustrant des séquences d'installation et de désinstallation d'une application de sécurité sur une carte collectrice insérée dans un dispositif d'accès conditionnel selon un mode  
5 de réalisation possible pour l'invention ;

- les figures 13 à 18 illustrent la structure des trames de communication utilisées avec un dispositif d'accès conditionnel conforme à un mode de réalisation possible de l'invention.

10

*Exposé détaillé de différents exemples non  
limitatifs de réalisation de l'invention*

L'appareil selon l'invention sera décrit sous forme  
15 d'une souris à bille, la même démarche s'appliquant pour les autres types de dispositifs de pointage. La figure 1 montre un appareil selon l'invention dérivé d'une souris opto-mécanique dont la bille (3) est retenue dans sa cage par le couvercle (2). Un clavier (6) est logé dans un dégagement  
20 prévu sur le corps inférieur (1) de la souris. La profondeur de ce dégagement est choisie en fonction de l'épaisseur du clavier et de l'épaisseur des pastilles glissantes (4) afin que l'ensemble ne touche pas la surface d'appui entraînant la bille (3).

25 L'appareil représenté dans la figure 1 comporte un coupleur de carte à microcircuit. Dans la figure 1, une carte à microcircuit (5), par exemple conforme à la norme ISO 7816 ou encore une carte sans contact, est introduite dans l'appareil par une fente latérale prévue en ce sens.  
30 L'appareil peut comporter des moyens pour accepter les deux types de carte à microcircuit, pour identifier le type de carte et vérifier son insertion correcte.

Ainsi, le clavier (6) peut être placé sur le couvercle supérieur de la souris, protégé ou non par un cache  
35 articulé. Ce dispositif peut comporter un afficheur (7) à cristaux liquides pour le contrôle des transactions et

opérations et il est connecté à l'équipement hôte par un cordon de liaison muni d'une prise pour le branchement sur le port ad-hoc de l'équipement hôte. L'alimentation du dispositif est fournie soit par une source autonome soit par  
5 l'équipement hôte. L'alimentation électrique peut être réalisée soit par une alimentation indépendante propre au périphérique, ou dans la plupart des cas, par la tension disponible sur le port (RS232, USB, GEOPORT, ...) auquel est relié le périphérique, ou un second port (clavier, ...).

10 L'appareil peut comporter une horloge à alimentation permanente nécessaire pour dater des transactions financières. L'appareil peut comporter aussi des moyens sécurisés habilités à recevoir une application porte-  
monnaie électronique. Ainsi il peut recevoir et conserver  
15 l'argent ou la valeur électronique. Lesdits moyens peuvent être réalisés soit avec un microcontrôleur en version sécurisé et comprenant une application porte-monnaie électronique, soit en utilisant un second coupleur de carte à microcircuit comportant une application porte-monnaie  
20 électronique. Cette deuxième carte porte-monnaie électronique est de préférence une carte miniature à contacts (5a) et logée à l'intérieur du dispositif (par exemple de format GSM, 15 x 25 mm). Ceci facilite son remplacement en cas d'expiration de validité ou de défaillance. Cette fonction  
25 financière intrinsèque correspond à un portefeuille électronique.

Une variante représentée en figure 2c consiste à remplacer le clavier de saisie des données personnelles par un équivalent informatique. Cet équivalent est constitué par  
30 un programme provoquant l'affichage sur l'écran (50) de l'équipement hôte d'une représentation graphique d'un clavier virtuel (54) composé de touches virtuelles (51, 52). Les touches virtuelles (51) de ce clavier sont positionnées de façon aléatoire et différente à chaque nouvelle activation de  
35 ce programme. La saisie des données personnelles s'effectue à l'aide des fonctions de pointage du dispositif d'accès

conditionnel selon l'invention. L'exploitation des signaux de positionnement et de validation de la position de l'index (53) sur le clavier virtuel (54) se fait exclusivement dans le périphérique, d'une manière empêchant la transmission des données de position validées à l'équipement hôte.

Plusieurs configurations ergonomiques sont possibles pour le boîtier (1) de la souris.

On a illustré sur les figures 2a et 2b deux configurations différentes envisageables.

Dans les deux cas, la fente (1b) est ménagée sur le bord du boîtier (1) le plus éloigné des touches d'actionnement de la souris, ces touches ayant été référencées par (8) sur ces figures 2a et 2b.

La configuration illustrée sur la figure 2b est avantageuse car elle permet de simplifier l'outillage de fabrication. La fente (1b) y est située au niveau de la rainure (1c) que présente habituellement une souris sur son pourtour dans le prolongement de l'espace entre ses touches d'actionnement (8) et le corps du boîtier (1).

La figure 3 illustre une configuration avantageuse à l'intérieur du boîtier (1). On sait que classiquement, il est prévu dans un boîtier de souris à bille deux axes encodeurs (41, 42) et un galet presseur (43) en contact permanent avec la bille (3). Ces axes encodeurs (41, 42) permettent de suivre les déplacements de la bille. Le ressort qui maintient le galet (43) en contact avec la bille (3) est un ressort (44) en spirale, ce qui permet de réduire l'encombrement du mécanisme de pression à l'intérieur, et donc de libérer un volume au niveau de la zone d'introduction de la carte à puce (5).

Dans une autre variante de souris à bille conforme à l'invention illustrée par les figures 4 à 6, le clavier (6) est disposé sur la face supérieure de la souris, c'est-à-dire sur la face qui est opposée au fond (1b). Un couvercle articulé (9) permet de protéger le clavier lorsque la fonction de coupleur de carte à puce n'est pas utilisée. Ce

couvercle (9) est représenté arraché sur la figure 4. Il présente une forme telle que sa face supérieure prolonge très exactement la forme du boîtier lorsqu'il est en position fermée, le périphérique se présentant alors comme une souris  
5 classique.

Ce couvercle (9) est articulé sur le boîtier (1) par l'intermédiaire d'un bras (10) par rapport auquel il est monté pivotant, ledit bras (10) étant lui-même monté pivotant, par rapport au boîtier (1) autour d'un axe  
10 parallèle à l'axe de pivotement du couvercle (9) sur ledit bras (10).

Une butée (10a) est prévue sur le boîtier (1) pour limiter le débattement du couvercle (9). On dispose ainsi d'une articulation qui permet à l'opérateur de dégager  
15 totalement le couvercle (9) par rapport à la zone occupée par le clavier (6), pour libérer l'accès de celui-ci, tout en conservant au périphérique un aspect compact.

Dans le cas d'une application à des transactions financières sur des réseaux en ligne et/ou en mode local, l'actionnement du clavier du périphérique par l'opérateur  
20 peut permettre les différentes opérations suivantes :

- Validation,
- Correction, effacement de la dernière entrée numérique,
- 25 • Journal, lecture de la liste des dernières transactions,
- Balance, lecture de la somme ou valeur restant dans la carte porte-monnaie électronique,
- Sélect, sélection de devise pour un porte-monnaie  
30 électronique intersectoriel,
- Annulation, abandonner la transaction courante,
- Local, arrêter la communication avec l'équipement hôte,
- Verrouiller, une carte à puce,
- 35 • EW/Carte, sélection portefeuille (EW) ou carte insérée, si applicable,

- Transfert, lancer une opération de transfert.

L'appareil attaché à un équipement hôte comportant des moyens logiciels adéquats et connecté à un réseau télématique, permet le paiement sécurisé en ligne des biens et services par cartes à puce bancaires et cartes porte-monnaie électronique, mais aussi le transfert sécurisé d'argent entre deux objets financiers distants.

Par exemple, deux personnes situées dans des localités différentes, possédant chacune un ordinateur personnel avec modem appareil selon l'invention peuvent exécuter les transactions sécurisées suivantes :

- transférer une somme d'argent de la carte bancaire de la première personne sur la carte porte-monnaie électronique de l'autre personne ;
- choisir la devise qui fera l'objet du transfert ;
- transférer une somme d'argent d'une carte porte-monnaie électronique à l'autre.
- Aussi, chacune des deux personnes peut utiliser les services financiers en ligne offerts par sa banque pour les cartes porte-monnaie électronique :
- transférer de l'argent de son compte courant sur une carte porte-monnaie électronique et réciproquement ;
- changer une somme d'argent en devise et réciproquement.

Chaque fois que l'identification du porteur de la carte est exigée, le code personnel ou la signature servant d'identificateur, sont saisis au niveau du dispositif qui crée ainsi une barrière à la fraude informatique.

L'appareil comportant de plus les moyens pour utiliser les cartes porte-monnaie électronique permet les opérations suivante :

- vérifier la valeur restante ou la balance ;
- la lecture du journal des transactions ;
- verrouiller son porte-monnaie électronique.

Une carte à puce 5 peut comporter plusieurs applications financières, par exemple une CB et au moins un porte-monnaie électronique. Tout appareil de base selon

l'invention comporte les moyens pour effectuer des transactions entre les applications financières résidentes sur une même carte à puce, les conditions de sécurité étant assurées implicitement par la carte même.

- 5 L'appareil comportant soit un portefeuille électronique (EW) interne, soit deux coupleurs identiques dont un comprenant une carte porte-monnaie électronique ayant rôle d'intermédiaire, peut être utilisé en mode local de fonctionnement pour des transactions carte à carte, les cartes
- 10 insérées successivement dans le connecteur disponible :
- débiter une carte bancaire et charger un porte-monnaie électronique ;
  - transférer de l'argent d'un porte-monnaie électronique à un autre ;
  - 15 • conserver de l'argent dans le portefeuille EW ;
  - annuler la dernière transaction.

On remarquera que les moyens mettant en oeuvre l'identification du porteur de la carte (saisie de code personnel ou signature), les moyens coupleurs de carte à puce

20 et les moyens de pointage (sélection, validation, modification) définissent la configuration de base pour chacun des types d'appareil décrits ci-dessus. Partant de chaque configuration de base ci-dessus, en combinant les différents moyens de communication série avec l'équipement

25 hôte, claviers, affichages, alimentations, horloge, portefeuille électronique, on obtient des familles d'appareils selon l'invention.

Un appareil périphérique du type de celui qui vient d'être décrit apporte à un ordinateur personnel ou une

30 télévision interactive les fonctions d'un terminal pour cartes à puce utilisables dans des applications financières, contrôle d'accès, identification et péage.

Il permet le paiement des biens et services sur les réseaux en ligne avec des cartes à puce bancaire (CB)

35 ou porte-monnaie électronique ainsi que des fonctions de banque à domicile. En versions à portefeuille électronique

(EW), l'appareil même peut servir comme réserve d'argent pour le paiement sur les réseaux en ligne ou en mode local.

L'appareil permet l'utilisation des moyens de paiement personnalisés (CB, porte-monnaie électronique, WE) ou anonymes (porte-monnaie électronique, WE). Ainsi, l'appareil permet la manipulation de l'argent électronique en tant que remplacement direct de l'argent physique et efface les barrières de la distance physique entre les opérateurs.

L'appareil peut aussi servir pour l'administration des réseaux d'entreprise, accès sécurisé aux ordinateurs, protection logicielle.

L'appareil remplace la souris habituelle ou tout autre dispositif série de pointage et il est accompagné d'un pilote logiciel adéquat à chaque type d'équipement hôte. Généralement, l'appareil est une télécommande destinée aux terminaux multimédia le reconnaissant comme dispositif de pointage (ordinateurs personnels, télévisions multimédia interactives, etc.). Il peut aussi comporter des applications additionnelles comme calculatrice financière, presse-papiers, agenda, etc.

Décliné sous la forme d'un presse-papiers à stylet et à double interface de carte à puce qui en option enregistre des fiches manuscrites compressées dans une mémoire, l'appareil pourra également avantageusement être utilisé par des professionnels de santé.

On a illustré sur la figure 7 une configuration pour la mise en oeuvre d'un contrôle biométrique, par exemple par un contrôle au moyen d'un scanner d'empreintes digitales ou d'un scanner de fond de l'oeil, comportant un capteur d'images (15), qui est par exemple un scanner d'empreintes digitales ou un scanner de fond de l'oeil, est relié au microcontrôleur du périphérique (13) sur cette figure 7. Ce microcontrôleur (13) est également relié aux moyens spécifiques de pointage (11), à l'écran d'affichage (7) ainsi qu'au clavier (6).

Le microcontrôleur (12) regroupe les moyens de contrôles de traitement et de communication de l'ensemble du dispositif. Ainsi il communique avec une carte à puce externe (5) par le biais de l'interface (13) et avec la carte à puce interne (5) par le biais de l'interface (14) et d'autre part avec le micro-ordinateur (19), auquel ledit périphérique est associé.

En variante encore, le microcontrôleur (12) est également avantageusement relié à un processeur de synthèse et de reconnaissance vocale (16) qui est par exemple lui-même relié à un microphone MIC et à un haut-parleur HP disposé dans le boîtier (1). Une variante de mise en oeuvre consiste à vérifier la signature vocale de l'utilisateur au moment de la lecture d'informations affichées sur un écran du périphérique ou de l'équipement hôte. Ce mode de réalisation permet d'effectuer la reconnaissance vocale et la comparaison avec la signature vocale numérisée enregistrée dans une carte à microcircuit (5) à partir d'un nombre très réduit de mots, et d'utiliser des algorithmes et circuits intégrés simplifiés et peu coûteux sans réduire de façon significative la sécurité de la comparaison.

Les moyens de traitement que constitue l'unité (12) mettent en forme l'objet biométrique relevé par le capteur (15) et/ou l'unité de reconnaissance vocale (16), pour permettre son traitement par une carte (5). Celle-ci reçoit et compare l'objet biométrique avec la référence qu'elle présente en mémoire. En variante, la comparaison entre la référence et l'objet biométrique relevé par le capteur (15) ou l'unité (16) peut être réalisée par le microcontrôleur (12).

On observera que les moyens de traitement que constitue microcontrôleur (12) peuvent être un coprocesseur mathématique optimisé pour le traitement des signaux et/ou les calculs cryptographiques. Aussi, tout ou partie de l'unité (16) peut être avantageusement intégré sur une même puce ou module (12).

L'objet biométrique, tel que l'image relevée par le capteur (15) ou la reconnaissance vocale que réalise l'unité (16), se substitue au code d'identification de l'utilisateur, qui n'a pas besoin d'entrer un code sur le clavier (6).

5 La figure 8 représente une configuration où le capteur (15) est situé sur un bord latéral du boîtier (1) de la souris. Ce bord présente un guide (17) destiné à recevoir un doigt de l'opérateur, par exemple son pouce. Le projet de norme européenne EN 1546 présente en détail le fonctionnement  
10 et l'utilisation des cartes porte-monnaie électronique. Le projet de norme européenne EMV décrit en détail le standard des procédés de paiement par cartes à microcircuit ainsi que les caractéristiques de telles cartes.

Le périphérique peut comporter des moyens de  
15 communication série sans fil pour augmenter sa mobilité par rapport à l'équipement hôte. Des moyens radio ou infrarouge peuvent être utilisés pour satisfaire les contraintes environnementales et celles des équipements hôtes ciblés.

Le périphérique peut encore être intégré au micro-  
20 ordinateur lui-même. Une variante en ce sens a été illustrée sur la figure 9. Dans cette variante, un micro-ordinateur présente un dispositif tactile de pointage (20). Un clavier (6) indépendant du clavier C de l'ordinateur est intégré au support S sur lequel clavier C et le dispositif tactile de  
25 pointage (20) sont montés.

Avantageusement, la surface tactile du dispositif (20) est également utilisée pour réaliser le clavier (6) de saisie des informations personnelles, une représentation dudit clavier étant superposée à ladite surface tactile.  
30 Cette représentation peut être visible en permanence. En variante, elle peut être visible seulement lors de l'opération d'identification du porteur, par exemple par un rétro-éclairage réalisé au moyen d'un film électroluminescent.

35 Une autre variante de réalisation d'un dispositif selon l'invention, met en oeuvre des moyens de synthèse

vocale et un dictionnaire adéquat. Ce dictionnaire peut être téléchargé et/ou modifié par une procédure sécurisée à partir d'un serveur accrédité. Ce serveur peut être par exemple celui du fabricant du dispositif d'accès conditionnel. Ce  
5 dernier peut, avec des moyens de reconnaissance vocale, apprendre un minimum de commandes requises par le déroulement des transactions, tels que par exemple : accepter, annuler, continuer. A titre d'exemple, pour le contrôle du prix affiché sur l'écran de l'ordinateur de 198,25 \$, le procédé  
10 consiste à transmettre l'information relative au prix périphérique qui transforme cette information par ses moyens de synthèse et reproduction vocale, pour émettre les sons "un", "neuf", "huit", "virgule", "deux", "cinq" et "dollars".

Ensuite le dispositif valide le prix pour la  
15 transaction par exemple à la commande "accepter" prononcée oralement par le titulaire de la carte à microcircuit introduite dans le dispositif. Les commandes vocales peuvent être enregistrées.

On se réfère maintenant aux figures 10 et suivantes  
20 sur lesquelles on a illustré d'autres aspects de l'invention.

Le périphérique comporte une application de sécurité, désignée par SAM dans la suite du texte. Par application de sécurité ou SAM, on entend un objet logiciel comportant un code exécutable et toutes les ressources  
25 spécifiques nécessaires à son fonctionnement, résidant et s'exécutant dans la mémoire d'un microcircuit sécurisé muni d'un système d'exploitation sécurisé aussi. Un exemple typique de SAM est le porte-monnaie électronique disponible sur carte à microcircuit. Il est prévu dans le périphérique,  
30 pour au moins un logiciel applicatif de l'équipement électronique hôte avec lequel ledit périphérique communique, une application de sécurité installée dans ledit périphérique.

L'applicatif et son application de sécurité  
35 connaissant chacun une même information secrète sous la forme

d'une ou plusieurs clés, il met en oeuvre un même algorithme cryptographique, permettant la vérification de cette clé.

On dispose ainsi d'une application de sécurité de distribution qui remplace la clé ordinaire de protection du logiciel applicatif contre les fraudes. Cette application de sécurité est avantageusement, mais non limitativement, portée par une carte à puce, désignée par la suite par carte collectrice SAMC. Cette carte collectrice est par exemple chargée à partir d'une deuxième carte appelée carte de distribution ou SAMD, qui est par exemple livrée avec le logiciel applicatif nécessitant une protection contre la fraude. Dans ce contexte, la figure 10 est un organigramme d'une séquence simplifiée d'interrogation d'une application de sécurité SAM résidant dans la carte collectrice d'un appareil périphérique par un applicatif s'exécutant localement ou accédant à l'équipement hôte qui communique avec le périphérique. La SAM a le rôle d'une clé de protection de cet applicatif. La première étape du test de la SAM (étape (101)) consiste à générer un code aléatoire (RNDC) qui est ensuite mémorisé. Dans une deuxième étape (102), ce code (RNDC) est crypté selon un procédé à clé symétrique bien connu dans l'art. Cette clé de cryptage est connue par l'applicatif et par sa SAM. Le résultat de l'étape (102) est un autre code représentant le test (CLG) à transmettre à la SAM. Dans l'étape (103), l'applicatif vérifie si il peut transmettre ce test (CLG) au pilote du dispositif. Dans l'étape (104), le message test (CLG) est transféré à ce pilote qui le transmet selon un protocole étendu du protocole de communication spécifique aux moyens de pointage dudit appareil périphérique à la SAM de destination.

Dans l'étape (105), l'applicatif attend pour un temps prédéfini la réplique de la SAM. La SAM utilise un algorithme pour décrypter le test (CLG). Si la SAM est authentique, la clé de décryptage est la même et retrouve-le code aléatoire initial en clair. Sa réplique (RPL) est transmise au pilote du dispositif pour être lue dans l'étape

(106) par l'applicatif. L'étape suivante (107) consiste à comparer le code initial (RNDC) avec la réplique (RPL). Si ils sont identiques, il n'y a pas de fraude. Une telle séquence de test de SAM s'intègre dans l'applicatif à  
5 protéger. Si la séquence de la figure 10 a un seul message de retour en cas de succès (108), les messages d'erreurs (109) sont plus nombreux dans la pratique et reflètent les situations d'échec possibles dans toutes ses étapes.

La séquence simplifiée d'installation d'une  
10 application de sécurité ou SAM dans le procédé selon l'invention est présentée dans la figure 11.

Une carte SAMD de distribution d'applications de sécurité peut servir pour plusieurs installations d'une même application de sécurité. Ladite carte comporte pour chaque  
15 application de sécurité un compteur de licences (LCNT) initialisé au nombre d'installation permise pour ladite application. Le programme d'installation de l'applicatif demande dans l'étape (110) la carte de distribution SAMD dans le coupleur de carte à puce du périphérique. La procédure est  
20 interrompue si :

- le test (111) ne reconnaît pas la carte de distribution SAMD ou le compteur du nombre de licences à installer LCNT est nul,
- le test (112) ne trouve pas assez de mémoire dans  
25 la carte collectrice SAM ou cette carte ne supporte pas la SAM à installer,
- le test (114) ne valide pas la copie.

Si les conditions (111) et (112) sont réunies, l'étape (113) transfère la SAM de la carte de distribution  
30 SAMD à la carte collectrice SAMC.

Le microcontrôleur du coupleur du périphérique déclenche ce transfert qui ensuite se déroule entre les deux cartes selon un quelconque procédé de transfert de données sécurisé.

35 Pendant ce transfert, Le microcontrôleur agit uniquement comme canal de liaison entre les deux cartes SAMC

et SAMD. Le système d'exploitation de la carte collectrice SAMC amène la SAM à sa forme exécutable. Ensuite, la carte SAMC effectue le test (114) qui comprend la validation du transfert proprement-dit et ensuite la vérification du fonctionnement correct de la SAM. Cette vérification consiste à simuler l'interrogation de la SAM et à vérifier son comportement. La carte collectrice SAMC efface de sa mémoire la SAM invalide. L'installation d'une SAM est équivalente à un transfert de valeur selon un mécanisme transactionnel similaire à celui utilisé dans les systèmes porte-monnaie électronique. Ce mécanisme transactionnel assure dans l'étape (115) que le compteur de licences (LCNT) est diminué d'une unité uniquement si la SAM est validée par les moyens sécurisés de stockage, gestion et exécution SAMC.

15 L'organigramme simplifié de désinstallation d'une application SAM dans le procédé selon l'invention est présenté sur la figure 12.

Le programme de désinstallation de l'applicatif protégé par une SAM demande dans l'étape (116) l'insertion de la carte de distribution SAMD ou équivalente dans le coupleur du périphérique. Le test (117) vérifie si la SAM à désinstaller accepte la carte introduite dans ledit coupleur. Si la carte SAMD est la carte d'origine, le code de la SAM y est toujours présent et l'étape (119) augmente d'une unité le compteur de licences (LCNT).

Si la carte SAMD n'est pas celle d'origine, le code de la SAM est transféré de la carte collectrice SAMC dans l'étape (121) à la condition (120) de mémoire suffisante, dans des conditions similaires à l'étape (113) du processus d'installation décrit ci-dessus. Toujours dans l'étape (121), le système d'exploitation de la carte SAMD crée un compteur de licences (LCNT) initialisé à zéro. Dans le cas de transfert de code de SAM, la carte SAMD vérifie dans l'étape (122) la validité de la copie, comme dans l'étape (114) de l'organigramme d'installation de SAM. Par un mécanisme transactionnel comme celui de l'installation d'une SAM,

l'opération de désinstallation assure que seulement en cas de succès la carte SAMD comporte une SAM valide et un compteur de licences (LCNT) incrémenté d'une unité et que la carte SAMC efface la SAM en question de sa mémoire dans l'étape 5 (123). Le procédé permet ainsi à toute carte SAMD ayant reçu par désinstallation une application de sécurité d'être équivalente à une carte de distribution d'origine. Une application de sécurité est transférée entre deux cartes 10 distantes qui communiquent entre elles par des moyens interposés assurant le transport et l'intégrité de leurs messages, via des réseaux de communication. Aussi, une procédure de transfert de SAM en tant que licence d'utilisation flottante d'un équipement hôte à un autre en utilisant les réseaux de communications est similaire à la 15 procédure de désinstallation de SAM décrite ci-dessus. Dans ce cas, la carte de distribution est remplacée par la carte collectrice de destination.

De préférence, le protocole de communication utilisé pour la gestion et l'exécution des applications de 20 sécurité utilise une même voie de communication série pour véhiculer l'information de pointage et les messages de sécurité. Ainsi, la fonction de pointage et la fonction de terminal de carte à microcircuit sont disponibles quasi simultanément et indépendamment l'une de l'autre. Dans le 25 cadre dudit protocole de communication, les informations et les commandes sont transmises sous la forme de trames comprenant un ensemble de champs constitué chacun d'une séquence codée comportant un nombre prédéterminé de bits, comme illustré dans la figure 13. Ainsi, une trame comporte 30 obligatoirement un champ d'identification (FID) et au moins un des champs suivants :

- champ de l'information de pointage,
- champ de l'information relative à une application de sécurité.

35 Le champ d'identification (FID) initialise les moyens de réception pour l'analyse de son contenu. Pour les

périphériques de pointage et un mode de fonctionnement donné, leurs trames ont une longueur fixe. Dans une telle trame, le bit de poids fort est réservé à l'identification de son début. Le protocole mis en oeuvre selon l'invention utilise  
5 la même méthode pour préserver la compatibilité avec les dispositifs de pointage classiques et place toujours l'information de pointage en début de trame étendue. Ainsi, il n'est pas restrictif de considérer la trame de pointage comme une part du champ d'identification (FID) de la trame  
10 étendue dont la figure 6 en est une illustration. Par exemple, la présence du champ de l'information relative à une application de sécurité peut être indiquée selon le même principe par une valeur particulière d'un groupe de bits du premier octet de la trame. Ainsi, le champ de l'information  
15 relative à une application de sécurité comporte tout ou une part des champs suivants dans l'ordre de citation, à partir d'une position déterminée par ladite valeur particulière d'un groupe de bits du champ d'identification (FID) :

- champ de contrôle (OPC),
- 20 - champ donnant la longueur du message d'application de sécurité (DLEN),
- champ qui comprend tout ou une part du message d'application de sécurité proprement-dit (CLG) ou (RPL),
- champ de contrôle de l'intégrité dudit message  
25 (CRC).

Les trames étendues ont une longueur variable selon le champ de contrôle (OPC). Si la trame comporte un message (CLG) destiné à une application de sécurité ou un message (RPL) destiné à un applicatif, le champ (OPC) est suivi par  
30 un champ (DLEN) donnant la longueur dudit message (CLG) ou (RPL). La longueur du champ (DLEN) est une fonction de la longueur maximale admise pour les messages (CLG) et (RPL). Les moyens de contrôle et traitement du dispositif selon l'invention ignorent la signification desdits messages (CLG)  
35 et (RPL). Le champ optionnel (CRC) permet l'éventuel contrôle de l'intégrité desdits messages (CLG) ou (RPL).

Une trame étendue est complètement définie par son champ de contrôle (OPC) qui comprend au moins les informations suivantes (figure 14) :

- le code (OPC.C) de l'opération concernant une ou  
5 plusieurs applications de sécurité,
- l'adresse de application de sécurité concernée  
par la trame (OPC.A),
- le nombre (OPC.S) d'octets du champ de  
l'information relative à une application de sécurité transmis  
10 par trame étendue, ce nombre (OPC.S) étant au moins égal à la  
longueur du champ (OPC).

L'adresse (OPC.A) prend aussi en compte le coupleur par lequel on accède à l'application de sécurité. Les messages longs sont transmis par segments de longueur  
15 constante (OPC.S) à l'exception d'un dernier segment, reparté sur plusieurs trames étendues plus courtes. Cette méthode permet d'assurer l'uniformité de la fréquence d'acquisition de l'information de pointage.

Les figures 15 à 18 illustrent une implémentation  
20 particulière de la structure des trames étendues décrites ci-dessus à l'aide des figures 13 et 14.

La figure 15 présente la trame émise par une souris conventionnelle. Cette trame comporte trois octets, dont les bits de poids fort ne sont pas utilisés. Ces bits sont  
25 utilisés pour indiquer les trames étendues.

En partant de cette trame, la figure 16 illustre la structure d'une trame étendue dont le champ d'identification (FID) reprend la trame de pointage et positionne à 1 le bit de poids fort de son premier octet. Ainsi, le pilote du  
30 dispositif détecte la trame étendue et analyse le quatrième octet qui correspond au champ de contrôle (OPC) de l'information de sécurité. Le cinquième octet (DLEN = m) indique la longueur en octets de la réplique (RPL) d'une application SAM, seul ou en association avec un autre champ  
35 binaire disponible dans les octets précédents, par exemple

les bits de poids fort des octets 2 et 3. Le champ de contrôle (CRC) comporte (n) octets.

Les figures 17 et 18 illustrent la structure de la première, respectivement la cinquième trame des trames étendues qui transmettent la réplique d'une application de sécurité en plusieurs segments consécutifs pour le paramètre OPC.S = 8, une réplique (RPL) de 32 octets et un (CRC) sur 16 bits. Le champ (OPC.S) indique au driver du dispositif le nombre d'octets du champ de l'information relative à une application de sécurité ajoutés à la trame de pointage, à l'exception d'une dernière trame. Aussi, les trames de pointage et les trames étendues peuvent être alternées.

L'invention est décrite dans ce qui précède à titre d'exemple non limitatif. Il est entendu que l'Homme du métier sera à même de réaliser diverses variantes sans pour autant sortir du cadre de l'invention.

**REVENDICATIONS**

1. Dispositif d'accès conditionnel destiné à être  
utilisé en liaison avec un équipement électronique hôte,  
constitué par un périphérique de pointage incorporant au  
5 moins un coupleur de carte à microcircuit,

caractérisé en ce qu'il incorpore en outre des  
moyens d'acquisition d'informations personnelles propres à un  
utilisateur et en ce que lesdites informations personnelles  
sont comparées localement avec les informations mémorisés  
10 dans la carte à microcircuit. (5) sans que lesdites  
informations personnelles ne transitent par l'équipement hôte.

2. Dispositif d'accès conditionnel selon la  
revendication 1, caractérisé en ce que les moyens  
15 d'acquisition d'informations personnelles propres à un  
utilisateur sont constitués par un clavier pour la saisie  
d'un code d'identification alphanumérique ou une tablette  
munie d'une zone sensible pour la saisie d'une information  
personnelle manuscrite.

20

3. Dispositif d'accès conditionnel selon la  
revendication 1 ou 2, caractérisé en ce que les moyens de  
saisie des informations personnelles sont constitués par un  
capteur pour la saisie d'un signal d'identification  
25 biométrique, tel qu'un capteur d'image d'empreintes digitales  
et/ou un capteur d'images de fond de l'oeil et/ou un capteur  
sonore associé à un moyen de reconnaissance vocale.

4. Dispositif d'accès conditionnel selon l'une  
30 quelconque des revendications précédentes, caractérisé en ce  
qu'il comporte un clavier (6) pour la saisie des informations  
personnelles et/ou un moyen d'affichage pour le contrôle de la  
transaction.

35 5. Dispositif d'accès conditionnel selon l'une  
quelconque des revendications précédentes, caractérisé en ce

que les moyens de saisie des informations personnelles sont constitués par un moyen propre à provoquer l'affichage sur l'écran de l'équipement hôte d'un clavier virtuel comportant des représentations graphiques dont la disposition varie aléatoirement à chaque activation desdits moyens, l'acquisition des informations personnelles s'effectuant par pointage des représentations graphiques et validation lors du positionnement du pointeur sur la représentation graphique recherchée, le traitement des informations de pointage et de validation sur l'écran virtuel étant réalisé dans le dispositif d'accès conditionnel exclusivement.

6. Dispositif d'accès conditionnel selon l'une quelconque des revendications précédentes caractérisé en ce que les moyens d'acquisition des informations personnelles sont constitués par un module d'acquisition et de numérisation de la voix de l'utilisateur.

7. Dispositif d'accès conditionnel selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens de synthèse vocale et de reproduction sonore pour le contrôle de la transaction.

8. Dispositif d'accès conditionnel selon l'une quelconque des revendications précédentes, caractérisé en ce que le moyen d'acquisition des informations personnelles est constitué par une zone tactile de pointage (11) comportant une représentation du clavier superposée à sa surface tactile.

9. Dispositif d'accès conditionnel selon l'une quelconque des revendications précédentes caractérisé en ce qu'il comporte une horloge à fonctionnement permanent et des moyens pour transmettre à l'équipement périphérique des données numériques datées comportant une séquence de données relative à l'autorisation calculée à partir des données

mémorisées dans la carte à microcircuit (5) et des données saisies par l'utilisateur et une séquence de données délivrée par l'horloge.

- 5                   10. Dispositif d'accès conditionnel selon l'une  
quelconque des revendications précédentes caractérisé en ce  
qu'il comporte les moyens lui permettant d'exécuter en  
coopération avec un équipement hôte, sur les réseaux en-  
ligne, toutes ou partie des transactions sécurisées suivantes  
10 impliquant une carte porte-monnaie électronique ou une carte  
bancaire : a) paiement, b) remboursement, c) annulation de  
l'opération, d) sélection de devise,  
et/ou toutes ou partie des transactions sécurisées  
suivantes impliquant la carte porte-monnaie électronique y  
15 insérée : e) chargement d'une carte porte-monnaie  
électronique à partir d'un compte bancaire, f) transfert de  
valeur d'une carte porte-monnaie électronique à un compte  
bancaire, g) transfert de valeur d'une carte porte-monnaie  
électronique à une autre carte porte-monnaie électronique, h)  
20 débiter la carte porte-monnaie électronique et créditer une  
carte bancaire.

11. Dispositif d'accès conditionnel selon l'une  
quelconque des revendications précédentes caractérisé en ce  
25 qu'il comporte les moyens lui permettant d'exécuter  
indépendamment et/ou en coopération avec un équipement hôte,  
toutes ou partie des opérations suivantes impliquant la carte  
porte-monnaie électronique qui y est insérée : a)  
vérification de la valeur actuelle ou la balance, b) lecture  
30 de la liste des transactions récentes ou journal, c)  
verrouillage de la carte porte-monnaie électronique, d)  
changement de code d'identification.

12. Dispositif d'accès conditionnel selon l'une  
35 quelconque des revendications précédentes caractérisé en ce  
qu'il comporte les moyens pour effectuer des transactions

entre les applications financières résidentes sur une même carte à microcircuit.

13. Dispositif d'accès conditionnel selon l'une  
5 quelconque des revendications précédentes caractérisé en ce  
qu'il comporte les moyens comprenant une application porte-  
monnaie électronique et les moyens lui permettant d'exécuter  
toutes ou partie des opérations suivantes entre cartes  
successivement insérées dans un même connecteur : a)  
10 transfert de valeur d'une carte porte-monnaie électronique à  
une autre carte porte-monnaie électronique, b) transfert de  
valeur d'une carte porte-monnaie électronique à l'appareil  
même, c) débiter ou créditer une carte porte-monnaie  
électronique et créditer ou débiter de la même valeur une  
15 carte bancaire, d) annulation de l'opération.

14. Dispositif d'accès conditionnel selon l'une  
quelconque des revendications précédentes caractérisé en ce  
que lesdits moyens comprenant l'application porte-monnaie  
20 électronique sont compris dans une carte à microcircuit (5)  
amovible.

15. Dispositif d'accès conditionnel selon l'une  
quelconque des revendications précédentes caractérisé en ce  
25 qu'il comporte en outre une surface active de numérisation à  
stylet et/ou tactile, et un afficheur, la surface active et  
l'afficheur étant superposés.

16. Procédé de sécurisation de l'accès à un  
30 équipement hôte, mettant en oeuvre un dispositif d'accès  
conditionnel conforme à l'une au moins des revendications  
précédentes caractérisé en ce que certaines des fonctions au  
moins dudit équipement hôte ne sont accessibles qu'après  
saisie par l'utilisateur d'une information personnelle  
35 conforme à une information enregistrée dans une carte à  
microcircuit et la vérification de la conformité entre

l'information personnelle et l'information enregistrée dans la carte à microcircuit est réalisée dans un périphérique relié à l'équipement hôte sans que l'information personnelle ne transite par l'équipement hôte.

5

17. Procédé de transactions informatiques sécurisées comportant une étape de comparaison entre une information personnelle de l'utilisateur et des données contenues dans une carte à microcircuit, mettant en oeuvre un  
10 dispositif d'accès conditionnel conforme à l'une au moins des revendications précédentes, caractérisé en ce que l'étape de contrôle est effectuée dans ledit dispositif d'accès conditionnel formant une barrière à la fraude informatique.

15

18. Procédé pour la gestion et l'exécution des applications de sécurité au sein d'un équipement électronique interactif munis d'un appareil périphérique, ledit équipement électronique comportant un écran et des moyens permettant l'exécution locale ou distante des logiciels applicatifs et  
20 ayant une interface utilisateur graphique comprenant des objets visuels sur lesquels un utilisateur agit manuellement par le biais dudit appareil périphérique

caractérisé en ce que ledit procédé comprend un protocole de communication entre une partie au moins des  
25 logiciels applicatifs et des moyens sécurisés de stockage, de gestion et d'exécution d'une application de sécurité coopérant avec au moins un coupleur destiné à recevoir notamment une carte à microcircuit (5) comportant une application de distribution des applications de sécurité, ce  
30 protocole étant une extension du protocole de communication spécifique aux moyens de pointage dudit appareil périphérique.

19. Procédé selon l'une quelconque des  
35 revendications 16 à 18, caractérisé en ce que les informations et les commandes sont transmises dans le cadre

dudit protocole de communication sous la forme de trames comprenant un ensemble de champs constitué chacun d'une séquence codée comportant un nombre prédéterminé de bits, chaque trame comprenant un champ d'identification (FID) et au

5 moins un des champs suivants :

- champ de l'information de pointage,
- champ de l'information relative aux moyens sécurisés.

10 20. Procédé selon la revendication 19, caractérisé en ce que le champ de l'information relative aux moyens sécurisés comporte tous ou une part des champs suivants dans l'ordre de citation :

- champ de contrôle (OPC),
- 15 - champ donnant la longueur du message d'application de sécurité (DLEN),
- champ qui comprend tout ou une part du message d'application de sécurité proprement dit (CLG) ou (RPL),
- champ de contrôle de l'intégrité dudit message
- 20 (CRC).

21. Procédé selon la revendication 20, caractérisé en ce que le champ de contrôle (OPC) comprend au moins les informations suivantes :

- 25 - le code (OPC.C) de l'opération concernant une ou plusieurs applications de sécurité,
- l'adresse de l'application de sécurité concernée par la trame (OPC.A),
- le nombre (OPC.S) d'octets du champ de
- 30 l'information relative à une application de sécurité transmis par trame étendue, ce nombre (OPC.S) étant au moins égal à la longueur du champ (OPC).

22. Procédé selon les revendications 16 à 21 caractérisé en ce que l'application de distribution des applications de sécurité (30) comporte un compteur de

licences (LCNT) pour le contrôle des transferts multiples d'une même application de sécurité dans la limite d'un nombre prédéfini d'installations ou licences.

- 5                   23. Procédé selon les revendications 18 et 22 caractérisé en ce que l'opération de transfert d'application de sécurité entre des moyens sécurisés locaux ou distants comporte toutes ou une part des étapes suivantes :
- 10                   - identification de l'initiateur du transfert,
- authentification réciproque des moyens sécurisés participants,
- copie sécurisée du code de l'application sur les moyens de destination,
- validation de la copie,
- 15                   - invalidation de l'application de sécurité dans les moyens source.

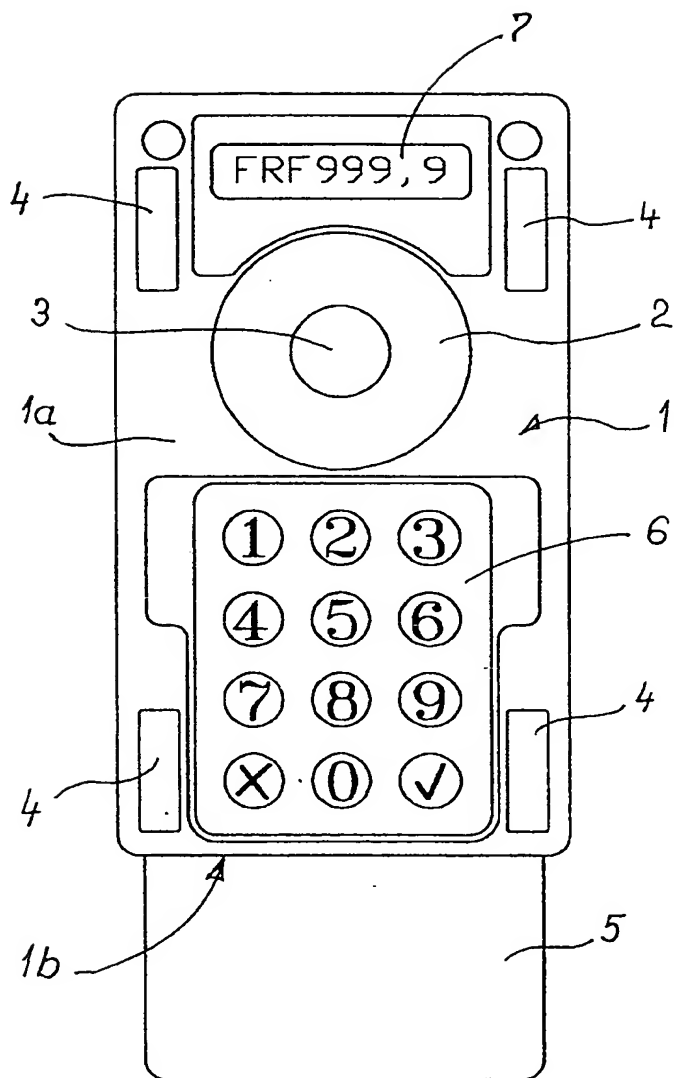
24. Procédé selon la revendication 23 caractérisé en ce que l'étape d'identification de l'initiateur du transfert consiste en ce qu'une application de sécurité installée dans un desdits moyens sécurisés de stockage, gestion et exécution des applications de sécurité (27) ou l'application de distribution des applications de sécurité (30), identifie l'initiateur du transfert par un code
- 20                   personnel saisi exclusivement avec les moyens dudit périphérique et sans que ce code transite par ledit équipement électronique interactif.

25. Procédé selon la revendication 24 caractérisé en ce que l'étape d'invalidation de l'application de sécurité dans les moyens source consiste dans l'effacement de son code et la libération de ses ressources à l'exception de l'application de distribution des applications de sécurité
- 30                   ..(30)..dont..seul le compteur de transferts (LCNT)..est
- 35                   décrémenté d'une unité.

## 33

26. Procédé selon l'une quelconque des revendications 16 à 25 caractérisé en ce que le driver du dispositif périphérique, fournit l'information de pointage à un logiciel applicatif et en même temps assure la  
5 transmission des messages vers le même ou un autre logiciel applicatif simultanément actif et son application de sécurité.

27. Procédé de sécurisation de l'accès à un  
10 équipement hôte selon l'une quelconque des revendications 16 à 26 caractérisé en ce que l'équipement hôte transmet au dispositif d'accès conditionnel des informations relatives à la transaction en cours, que ces informations sont traduites par synthèse vocale, et que la validation de la transaction  
15 soit réalisée par la prononciation orale d'un mot ou d'une locution prédéterminée par le titulaire de la carte à microcircuit introduite dans le dispositif.



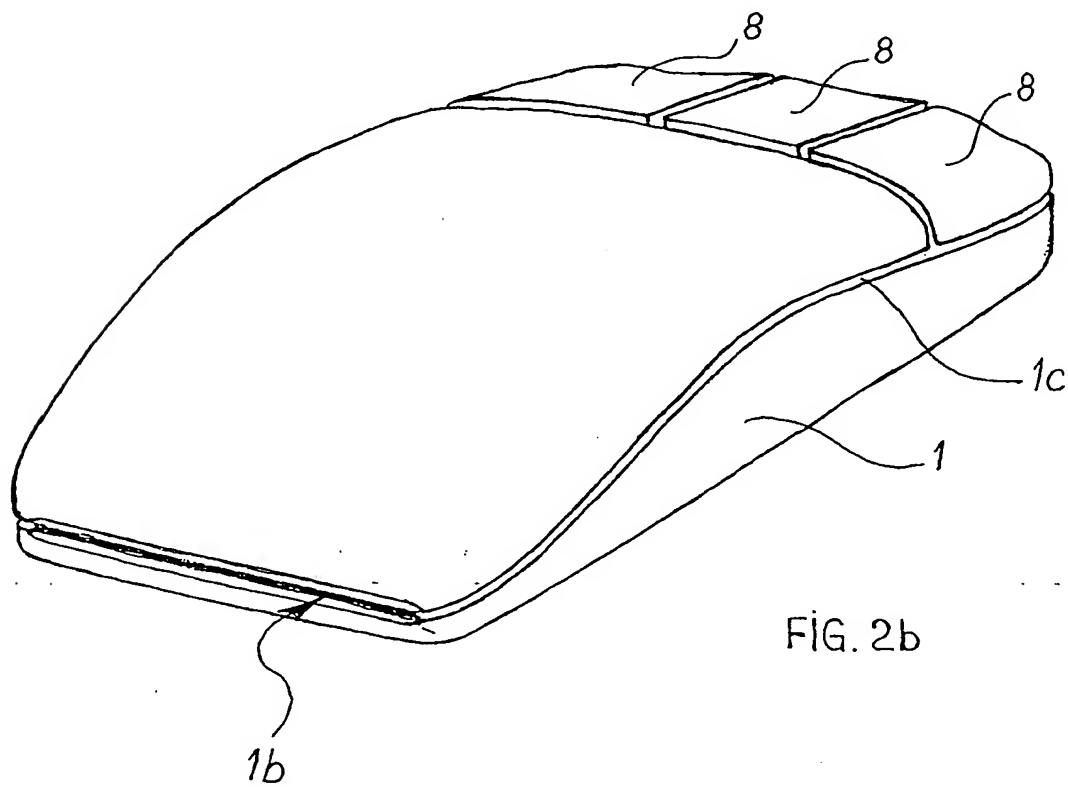
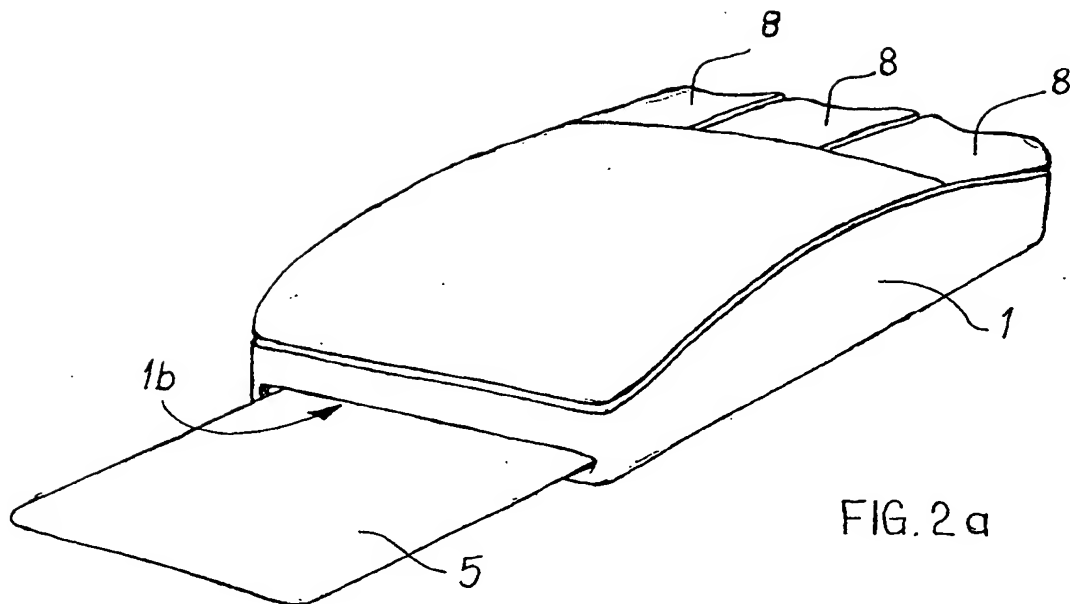
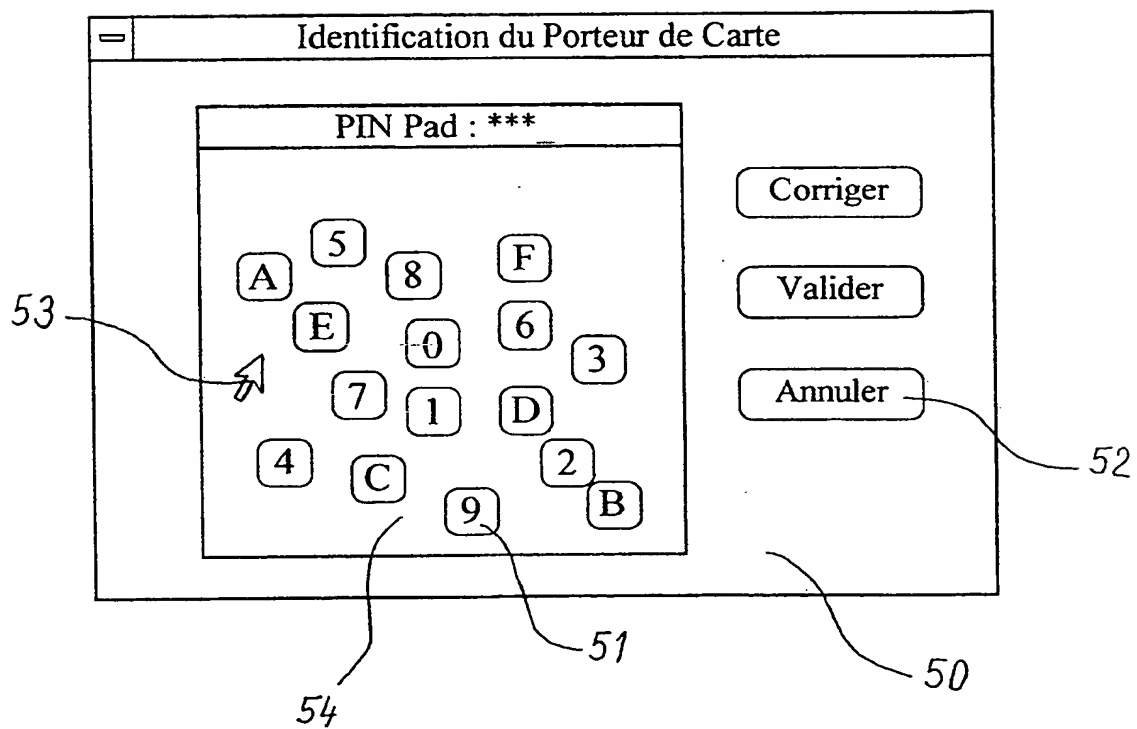


FIG. 2c



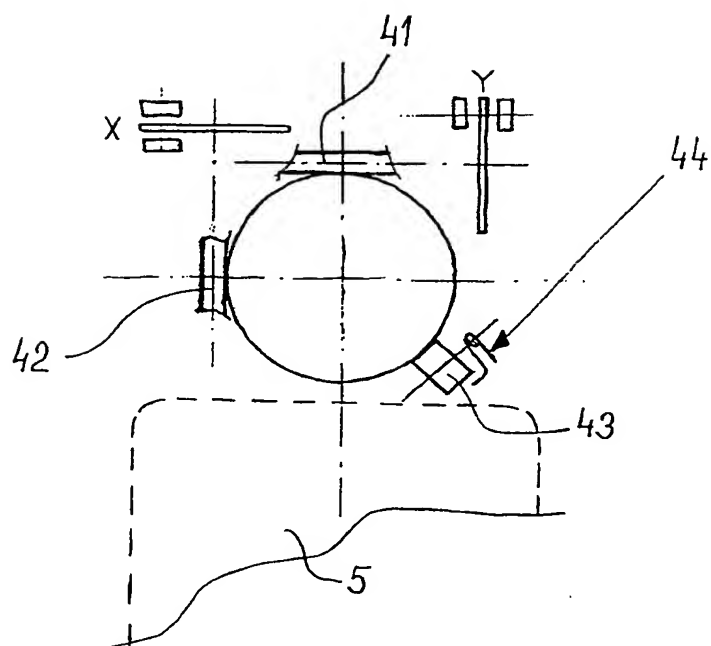


FIG. 3

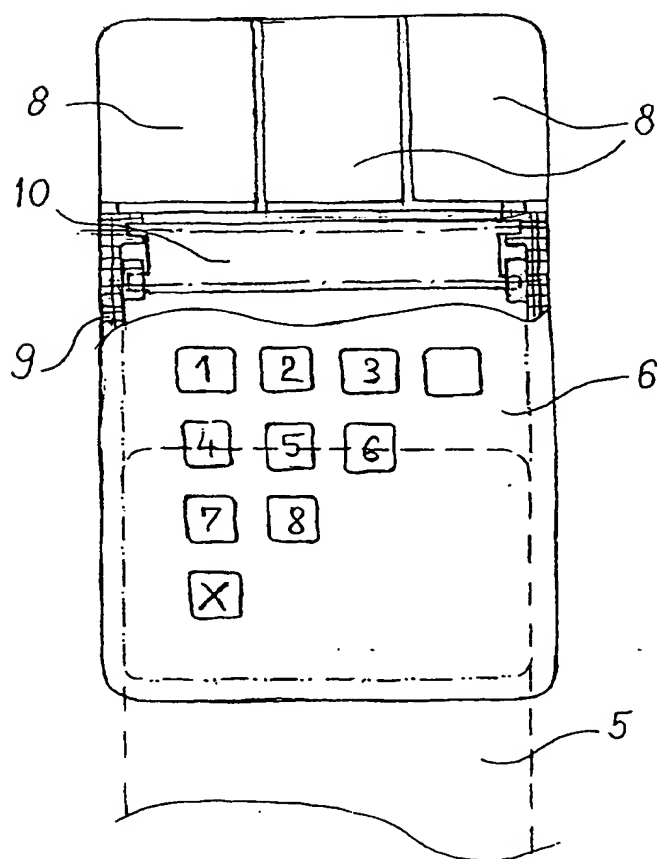
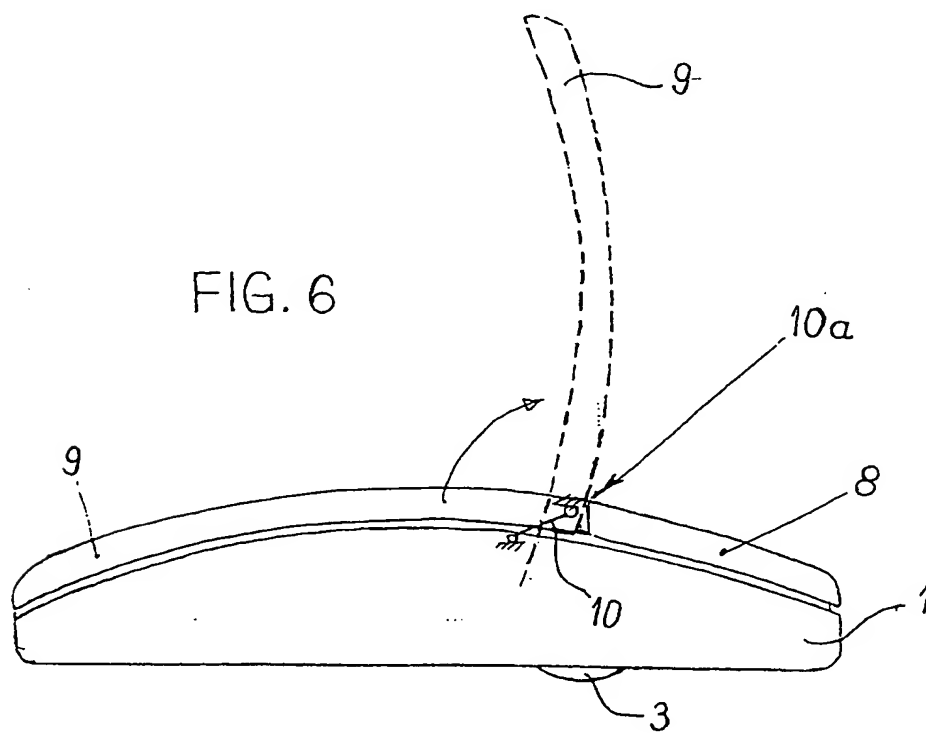
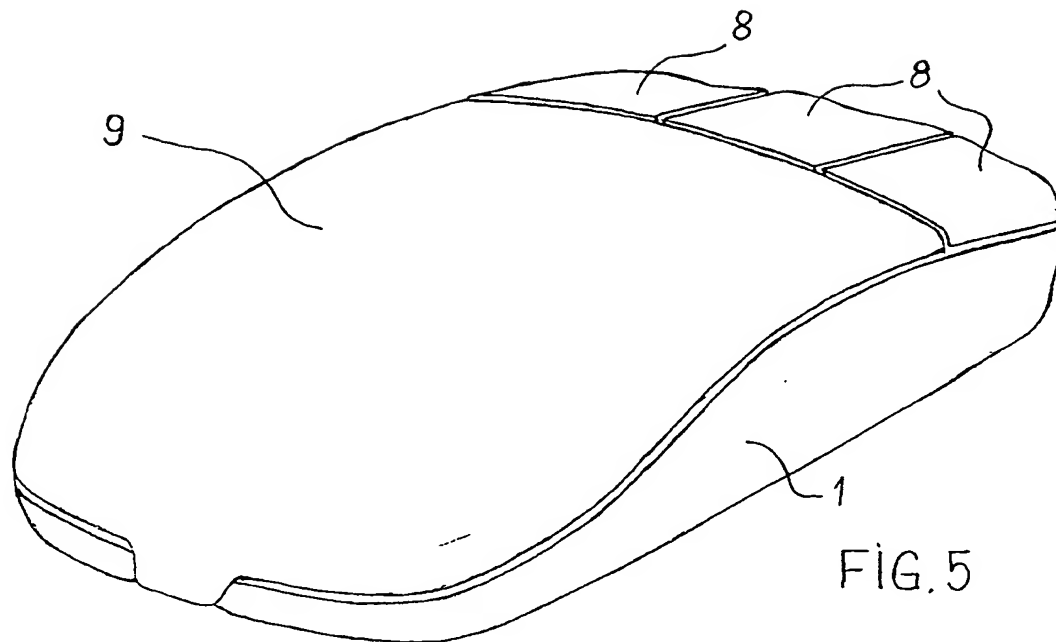


FIG. 4



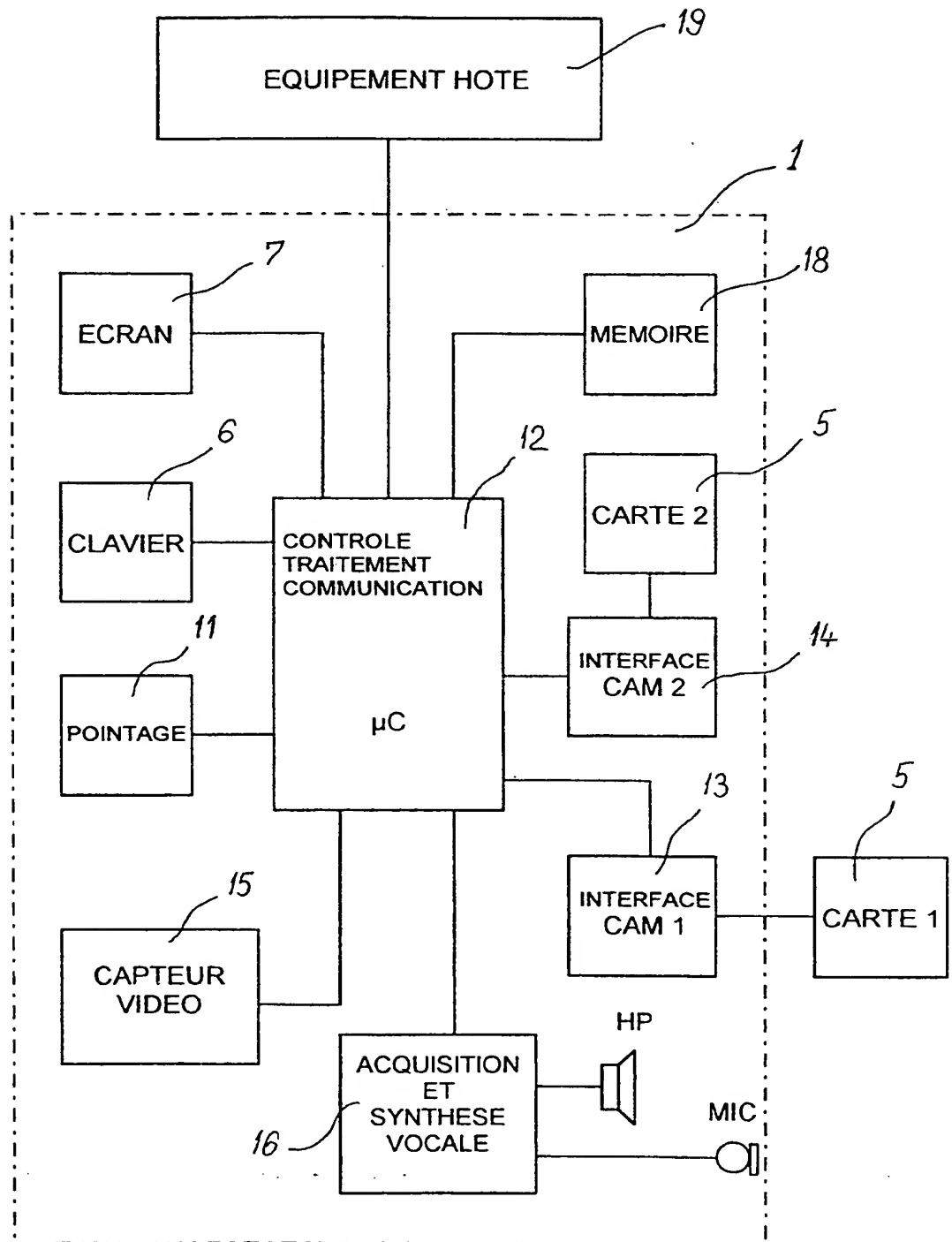
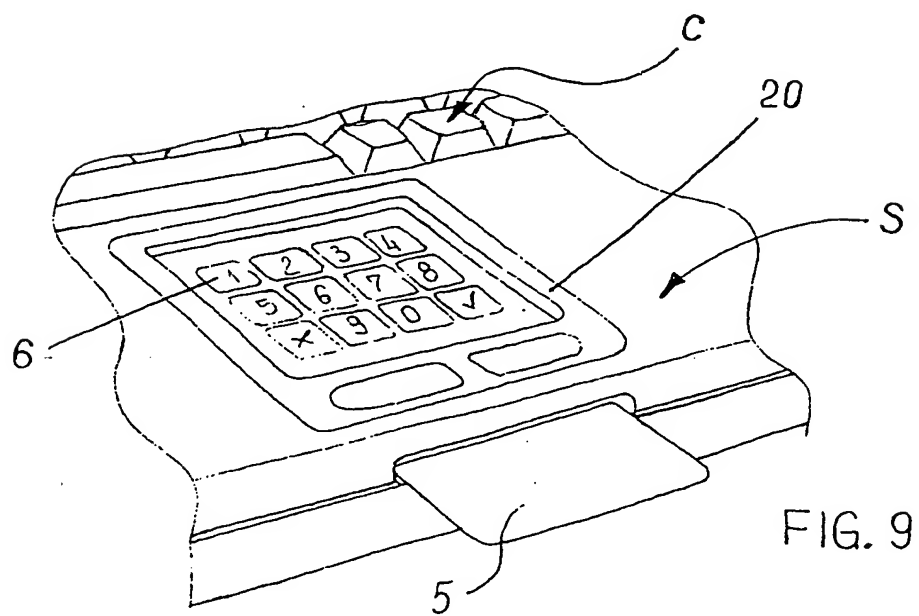
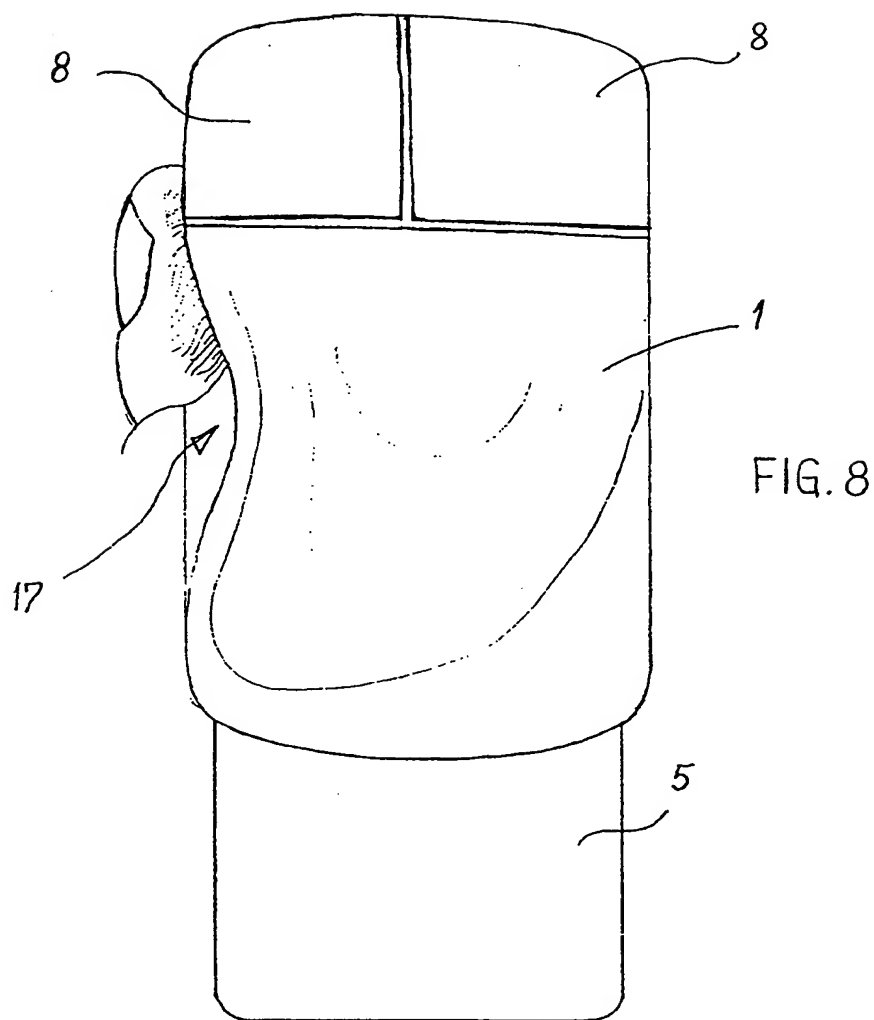


FIG. 7

7 / 12



8 / 12

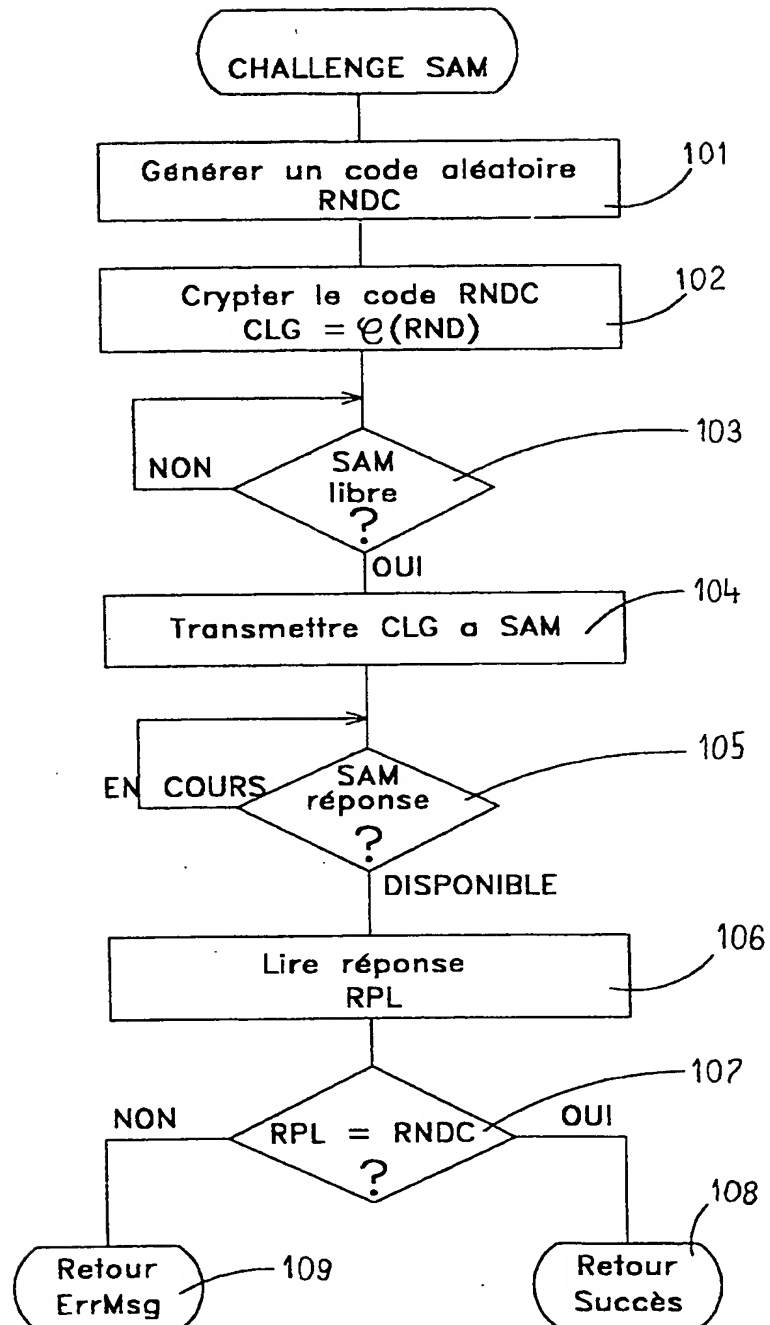


FIG. 10

9 / 12

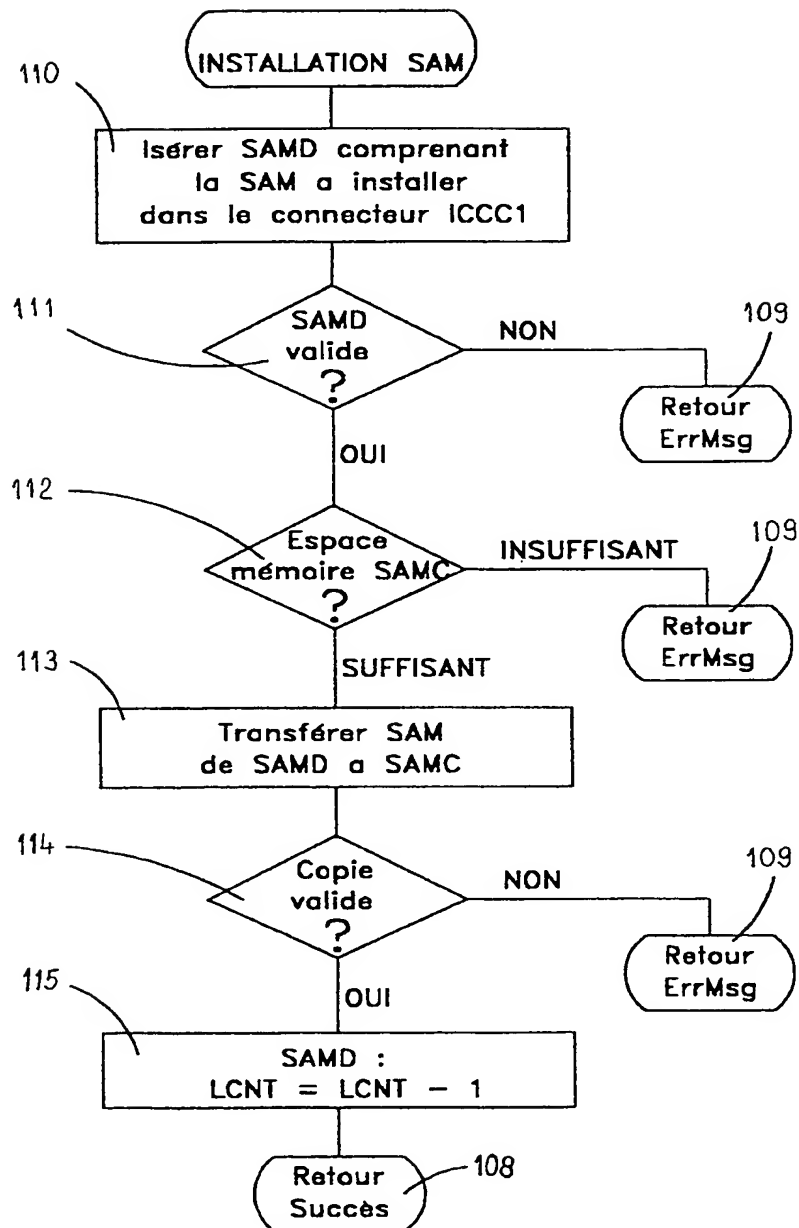


FIG. 11

10 / 12

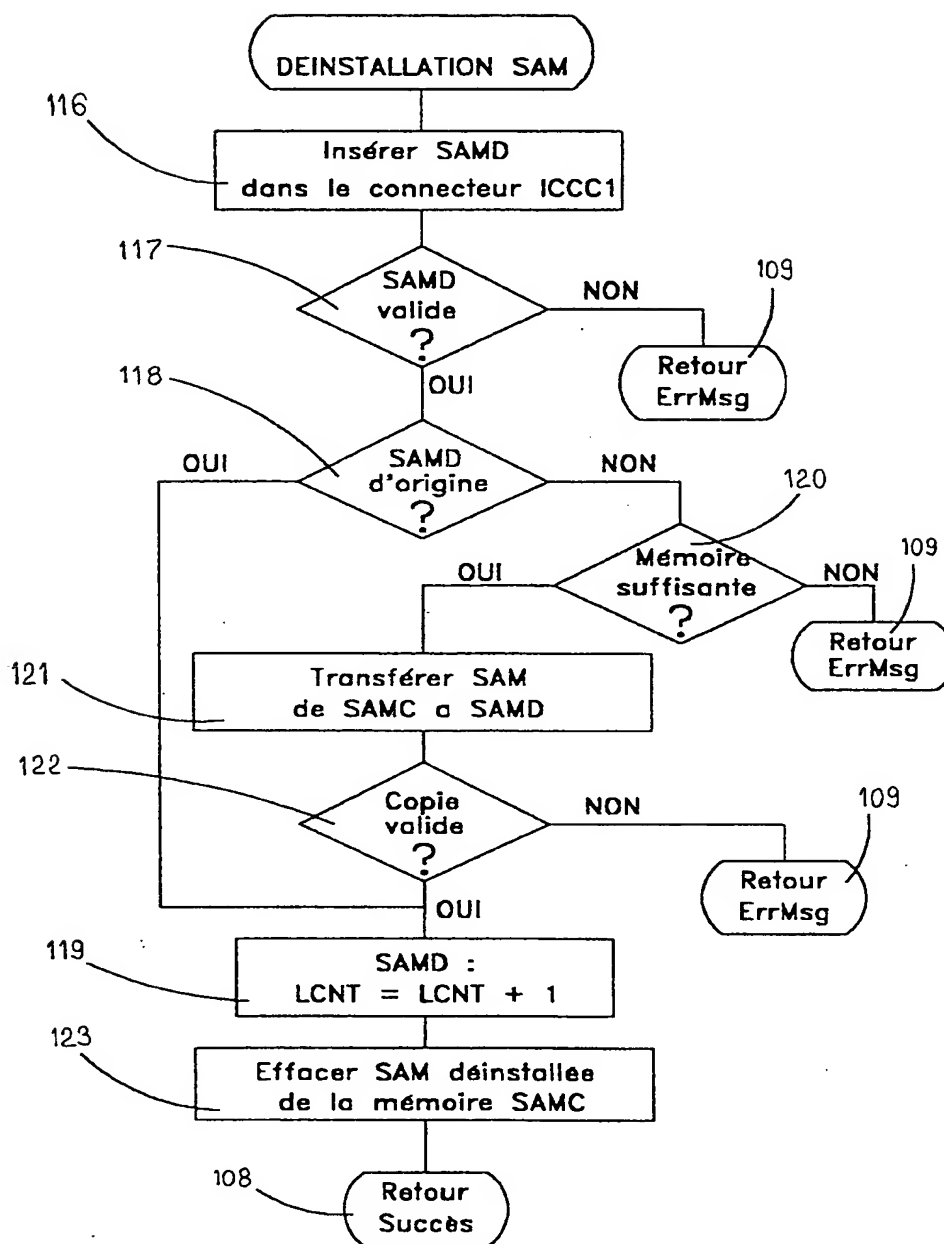


FIG. 12

11 / 12

FID	OPC	DLEN	CLG / RPL	CRC
-----	-----	------	-----------	-----

FIG. 13

OPC		
OPC.C	OPC.A	OPC.S

FIG. 14

Séquence	7 MSB	6	5	4	3	2	1	0 LSB
Byte 1	X	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0

FIG. 15

Séquence	7 MSB	6	5	4	3	2	1	0 LSB
Byte 1	1	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
Byte 4	OPC							
Byte 5	DLEN = m							
Byte 6	RPL <sub>m-1</sub>							
...	...							
Byte m+6	RPL <sub>0</sub>							
Byte m+7	CRC <sub>n-1</sub>							
...	...							
Byte m+n+6	CRC <sub>0</sub>							

FIG. 16

12 / 12

 $m = 32 ; n = 2 ; k = 8 ; FS_{00} ;$ 

Séquence	7 MSB	6	5	4	3	2	1	0 LSB
Byte 1	1	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
Byte 4	OPC							
Byte 5	DLEN = 32							
Byte 6	RPL <sub>31</sub>							
Byte 7	RPL <sub>30</sub>							
Byte 8	RPL <sub>29</sub>							
Byte 9	RPL <sub>28</sub>							
Byte 10	RPL <sub>27</sub>							
Byte 11	RPL <sub>26</sub>							

FIG. 17

 $m = 32 ; n = 2 ; k = 8 ; FS_{04} ;$ 

Byte 1	1	1	L	R	X7	X6	Y7	Y6
Byte 2	X	0	X5	X4	X3	X2	X1	X0
Byte 3	X	0	Y5	Y4	Y3	Y2	Y1	Y0
Byte 4	RPL <sub>01</sub>							
Byte 5	RPL <sub>00</sub>							
Byte 6	CRC01							
Byte 7	CRC00							

FIG. 18